Outlook Web Access

User Training

12/01/2006

Your Responsibility

- It is your responsibility as a Government representative to protect the DoD information that is entrusted to you.
- By using your home computer for OWA access you are expanding the Global Information Grid (GIG)
- Any vulnerabilities on your current system are now added to the GIG.
- The more secure your computer is, the less risk is added to the GIG.

Your Responsibility

- Remember that the software license to operate the CAC reader is the property on the Navy. At the termination of your employment:
  - Return all Government owned property to your command
  - Remove the CAC reader software from your home computer.

Outlook Web Access (OWA)

- Outlook Web Access (OWA) is a convenience to access e-mail from outside a network.
- All DoD Outlook web access, (OWA) is required to use CAC identity certificates for authentication, email signing and encryption.
- To access OWA from your Non-DOD computer you must install the CAC reader, software anti-virus protection and firewall. Please refer to the installation guide for further information.

OWA Access

- Remember that access to your OWA is a privilege not a right.
- If you do not protect your home computer, you are not protecting the GIG.
- A password protected screen-lock will be set to activate with 15 minutes of inactivity.

What is Spyware

- Spyware is a malicious program that aids in gathering information about a person or organization without their knowledge.
- Spyware can get in a computer by Web browsing, viewing an HTML email, or opening an attachment

How to avoid Spyware

- Do not open any email from someone you do not know.
- Don’t open attachments that you are not suspecting.
- Even if you know the sender verify that the email and attachment are valid prior to opening it.

If you think you have Spyware

- Run an immediate virus scan of your computer with the latest update.
- Both Symantec and MacAfee virus scan software contain the ability to detect Spyware.

Basic Security principles

- Use anti-virus software on your personal computer and keep it up-to-date
- Scan all files and email downloaded from the Internet
- Download operating system, software patches and updates regularly
- Install and use firewalls when connected to the Internet

Basic Security principles

- Backup Important files
- Use complex passwords at home, not just on DOD systems.
- Disconnect the computer from the internet when not on-line. Leaving your OWA session connected for extended periods of time, leave a door that a hacker can use to access the GIG.

Basic Security principles

- Use only a wired internet connection (i. e., Phone dial-up, cable or DSL modem).
- Ensure that no wireless connection is turned on during the duration of the session.
- Ensure that no other web browser connections are opened for the duration of the session.

Basic Security principles

- Clear your cache before logging off. (see slide regarding this operation)
- No peer-to-peer file-sharing software (examples are Skype, Kazaa. Morpheus, and Limeware) may be installed on your system.
- log off and either turn off or reboot your computer at the end of your session

Handling of Government Information

- **Key Policy Points**
  - All DON policies and instructions are to be followed to their full extent.
  - The following are illustrations of key points.
- Same policies and procedures apply as if you were at your command.
- Handle, store, maintain and destroy all classified information in accordance with DOD and DON policy.

Handling of Government Information

- Immediately notify your command of any information loss, theft or suspicious behavior of your system.
- Do not download any PII, FOUO or the C.U.I. data during your session.
- Do not leave data on your system.
- If you inadvertently saved any data to your computer (Electronic Spillage) contact your COMMAND IAM immediately.

Handling of Government Information

- As a government OWA user you agree to unlimited government monitoring of your email account either at work or at home.
- Any violation may result in disciplinary action
- Electronic Spillage may result in the loss of your personal hard drive or storage media.

Electronic Spillage

- Electronic Spillage is data placed on an information technology system possessing insufficient security controls to protect the data at the required classification (e.g.., such as Unclassified Naval Nuclear propulsion information (U-NNPI)) is introduced to a non DOD computer.
- No Personal Identifiable Information (PII) or CUI information is allowed to be processed on a non DOD computer other than the OWA user.

Electronic Spillage

- If PII or CUI information data is inadvertently placed on to the non DOD system, it can be removed (wiped) in two ways:
- 1)Delete the file from the system
  - Clear the unused portion of the storage media using a “shredded” utility such as BC Wipe
- 2)Use a “shredder” utility that will completely erase the file (by overwriting) from the storage media.

Clearing Data

- **Clearing**. Removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities
- When you delete files from a disk on your computer, Windows does not erase the contents of the files from the disk, it only deletes “references” to these files from the systems tables.
- The contents of the files remain on the disk and can be recovered using any recovery utility.

Anti-Virus

- In order to gain access to your Navy OWA account you are be required to install and use anti-virus protection and personal firewall software.
- It is your responsibility to:
  - install anti-virus software
  - configure anti-virus software.

Anti-Virus

- Update your current anti-virus files by downloading the updates at least weekly or when prompted. (recommend that auto-update be enabled)
- Scan for viruses weekly. (recommend that scheduled scans be enabled)

Firewalls

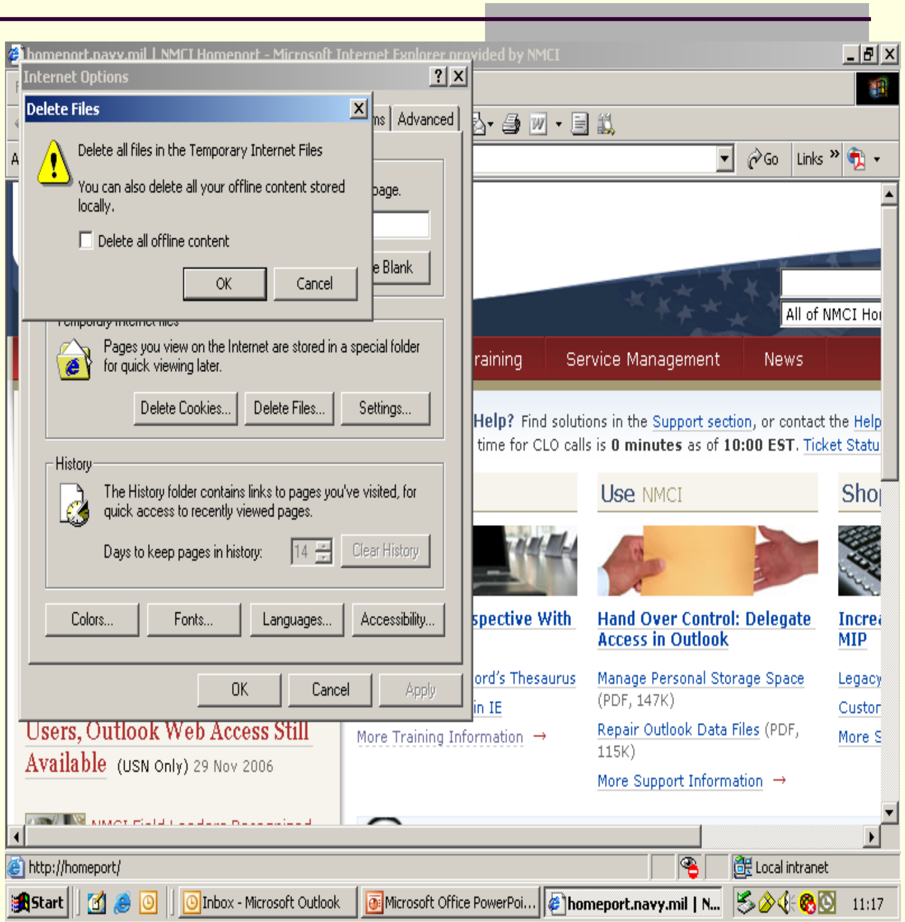
- Required on the computer accessing a DoD network via OWA.
- Protects your computer from network/hacker attacks
- Must contain “Port/Protocol” Filtering
- Must be configured to “deny all”, allow by exception.
- Approved software is available to all DoD employees at no cost from the DoD INFOSEC web

What is the cache

- A cache is a place where your computer stores information temporarily. The files you automatically request by looking at a Web page are stored on your hard disk in a cache subdirectory under the directory for your browser (for example, Internet Explorer).
- When you return to a page you've recently looked at, the browser can get it from the cache rather than the original server, saving you time and the network the burden of some additional traffic.

Clearing the Cache

- **Internet Explorer**
  - Open the **tools** menu and choose **Internet Options**
  - On the **General** tab, click on **delete files**… under **Temporary Internet Files**
  - Click **OK**



homeport.navy.mil | NMCI Homeport - Microsoft Internet Explorer provided by NMCI

Internet Options

Delete Files

Delete all files in the Temporary Internet Files

You can also delete all your offline content stored locally.

☐ Delete all offline content

Temporary Internet files

Pages you view on the Internet are stored in a special folder for quick viewing later.

History

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

Days to keep pages in history: 14

Help? Find solutions in the Support section, or contact the Help … time for CLO calls is **0 minutes** as of **10:00 EST**. Ticket Statu…

Users, Outlook Web Access Still Available (USN Only) 29 Nov 2006

Clearing the Cache

- **Netscape**
  - Open the edit menu and choose **Preferences**.
  - Click the **Advanced** Category.
  - Click on the **Cache** Category.
  - Click on the **Clear disk cache** button.
  - Click on the **Clear memory cache** button.
  - Click **OK**.

Ending your E-mail session

You must end your e-mail session by using the following steps:

1. Closing all DON e-mail files.
2. Clearing the web browser cache
3. Exiting and closing the browser.
4. Immediately turn off the computer, sleep and stand-by modes are **not** acceptable.

Close all Navy email files

- All email files are closed to avoid the possibility of inadvertently saving these files to your hard disk.
- Prevents unauthorized users, from viewing or copying this information.

Sleep/standby mode

- When a computer goes into sleep or standby mode, it shuts down the screen and disk drive.
- Once awakened, the computer returns to its former operating status Sleep mode is when you computer is saving energy.
- All information form previous sessions is still in cache and memory.

Turn off computer

- By turning off the computer you are clearing the memory of any residual data that may remain from you session.
- Clears any other temporary storage devices that may be contained in your machine.
- Prevents hackers from attempting to access your computer

Conclusion

- NMCI users can find further information on Homeport concerning Outlook web Access.